

# A Proof of the Erdős-Ulam Problem Assuming Bomberi-Lang Conjecture

Jafar Shaffaf

## Abstract

A rational set in the plane is a point set with all its pairwise distances rational. Ulam and Erdős conjectured in 1945 that there is no dense rational set in the plane. In this paper we associate special surfaces, we call them distance surfaces, to finite (rational) sets in the plane. We prove that under a mild condition on the points in the rational set  $S$  the associated distance surface in  $\mathbb{P}^3$  is a surface of general type. Also if we assume Bombieri-Lang Conjecture in arithmetic algebraic geometry we can answer the Erdős-Ulam problem.

AMS Subject Classification 2000: 14G05, 30D35, 52C10.

## 1 Introduction

A rational (respectively integral) distance set is a subset  $S$  of the plane  $\mathbb{R}^2$  such that for all  $s, t \in S$ , the distance between  $s$  and  $t$  is a rational number (respectively, is an integer). On any line, one can easily find an infinite rational set that is in fact dense. One can also easily find an everywhere dense rational subset of the unit circle. However it is not known if there is a rational set with 8 points in general position, that is, no 3 of them on a line and no 4 on a circle. In 1945, Anning and Erdős [AE] proved that any infinite integral set must be contained in a line. In 1945, Ulam conjectured that there is no everywhere dense rational set in the plane, see Problem III.5 in [G]. A deep conjecture of Erdős [E] states that an infinite rational set has to be very restricted.

Huff [H] considered rational distance sets  $S$  of the following form: given distinct  $a, b \in \mathbb{Q}^*$ ,  $S$  contains the four points  $(0, \pm a)$  and  $(0, \pm b)$  on the  $y$ -axis, plus points  $(x, 0)$  on the  $x$ -axis, for some  $x \in \mathbb{Q}^*$ . Such a point  $(x, 0)$  must then satisfy the equations  $x^2 + a^2 = u^2$  and  $x^2 + b^2 = v^2$  with  $u, v \in \mathbb{Q}$ . The system of associated homogeneous equations  $x^2 + a^2 z^2 = u^2$  and  $x^2 + b^2 z^2 = v^2$  defines a curve  $C(a^2, b^2)$  of genus 1 in  $\mathbb{P}^3$ . Huff [H] and Peeples [P] provided examples in which the elliptic curve  $C(a^2, b^2)$  has a positive rank over  $\mathbb{Q}$ , thus exhibiting examples of infinite rational distance sets that are not contained in a line or in a circle. These remain to this day the 'largest' known such examples. Assuming

Bombieri-Lang conjecture, in this paper we show that this is actually the largest possible example (see Corollary 1).

Using Mordell conjecture, proved by Faltings, J. Solymosi and F. De Zeeuw [SZ] proved that lines and circles are the only irreducible algebraic curves that contain an infinite rational set. They also showed that if a rational set  $S$  has infinitely many points on a line or on a circle, then all but 4 (respectively 3) points of  $S$  are on the line (respectively circle). This answers questions of Guy, Problem D20 in [G], and Pach, Section 5.11 in [BMP]. For a rational distance subset of the plane intersecting any line in finitely many points, it was shown in [MS] that there is a uniform bound on the number of these intersections. The main tool in [MS] is a conditional uniform boundedness theorem on the number of rational points of algebraic curves of genus  $g \geq 2$  on a fixed number field  $K$  ([CHM1]).

For one of our main results we need to assume the Bombieri-Lang Conjecture. The Lang Conjecture generalize the Mordell Conjecture to varieties of higher dimension. For a more complete discussion of Lang Conjectures see for example [L]. Analogous of the Mordell Conjecture for varieties of *general type* - a natural generalization of the notion of curves of genus  $g \geq 2$  to higher dimensions - is as follows (for the precise definition see for instance [L]):

**Weak Lang Conjecture.** Let  $X$  be a projective variety of general type defined over a number field  $K$ . Then the set of rational points  $X(K)$  is not Zariski dense in  $X$ .

It is worth mentioning one of the main consequences of the Weak Lang Conjecture in number theory and arithmetic geometry.

**Uniform Bound Theorem.** The weak Lang conjecture implies that, for every number field  $K$  and for every  $g \geq 2$ , there exists a number  $B(K, g)$  such that no curve of genus  $g$  defined over  $K$  has more than  $B(K, g)$  points defined over  $K$ .

For the main references of the Lang Conjectures and its consequences about the distribution of rational points on curves see [CHM1], [CHM2], [L] and [Ca2].

The result of this paper should be considered as a witness for the power of the Bombieri-Lang conjecture, rather than a real proof for this problem. However, to the best of our knowledge we are far beyond a proof of the Lang conjecture compared with the same conjecture for curves that is, Faltings Theorem (Mordell conjecture).

In this paper we associate a surface to a finite (rational) subset  $A = \{(\alpha_1, \beta_1), \dots, (\alpha_m, \beta_m)\} \subset \mathbb{R}^2$  as follows:

$$z^2 = \prod_{i=1}^m \{(x - \alpha_i)^2 + (y - \beta_i)^2\}, \quad (1.1)$$

and we call it distance surface. Also we will see that the points in the rational distance set play the role of the rational points on these distance surfaces over an appropriate number field.

The following theorem is one of our main result (see Section 3):

**Theorem 1** *Let  $m = 2g + 2$  be an even integer number with  $g \geq 2$  and assume  $A = \{(\alpha_1, \beta_1), \dots, (\alpha_m, \beta_m)\}$  be a finite subset of points in the plane not all on a line. Then the associated distance surface  $S$  (the projectivization of the equation (1.1) in  $\mathbb{P}^3$ ) is of general type.*

The above theorem is our key tool to deduce the following main result of this paper.

**Theorem 2** *Assuming Bombieri-Lang Conjecture, there is no dense rational distance subset in the plane.*

In the end, as a corollary of the proof of the above theorem we show that an infinite rational set in the plane should be very restricted.

**Corollary 1** *Let  $S$  be a rational set with infinitely many points not all on a line. Then all but at most 4 (3) points lie on a line (circle).*

The paper is organized as follows. In Section 2 we recall some preliminaries and known results about rational distance sets. In Section 3 we explain the construction of a special surface in  $\mathbb{P}^3$ , using a rational distance set for which the points in the rational set play the role of its rational points over an appropriate number field and we also prove Theorem 1.1. At the end, assuming the Bombieri-Lang conjecture in arithmetic algebraic geometry we answer the Erdős-Ulam problem.

## 2 Preliminaries and Known Results on Rational Distance Sets

Rationality of distances in  $\mathbb{R}^2$  is clearly preserved by translations, rotations, and uniform scaling  $((x, y) \rightarrow (\lambda x, \lambda y)$  with  $\lambda \in \mathbb{Q}$ ). We call a transformation  $T : \mathbb{R}^2 \rightarrow \mathbb{R}^2$  a similarity transformation if it can be written as the composition of translations, rotations and uniform scaling. Also rational sets are preserved under certain central inversions (an inversion with respect to a point in the rational set and with a rational radius), more precisely we quote the following lemma from [SZ].

**Lemma 1** *If we apply inversion to a rational set  $S$ , with the center  $x \in S$  and a rational radius, then the image of  $S \setminus \{x\}$  is a rational set.*

A priori, points in a rational set have arbitrary coordinates. However, after moving two of the points to two fixed rational points by translating, rotating and scaling, the points are almost rational points. The following simple lemma is well known (see [K]).

**Lemma 2** *For any rational set  $S$  there is a square free integer  $k$  such that if a similarity transformation  $T$  transforms two points of  $S$  into  $(0, 0)$  and  $(1, 0)$ , then any point in  $T(S)$  is of the form  $(r_1, r_2\sqrt{k})$ ,  $r_1, r_2 \in \mathbb{Q}$ .*

**Proof** Let  $(0, 0)$  and  $(1, 0)$  and  $(x, y)$  be members of the rational set  $S$ . Then we have  $x^2 + y^2 = q_1^2$  and  $(x - 1)^2 + y^2 = q_2^2$  such that  $q_1, q_2 \in \mathbb{Q}$ . By solving these two equations we have  $x = \frac{q_1^2 - q_2^2 + 1}{2}$ , and so  $x$  is a rational number. By substitution of the value of  $x$  and a simple manipulation for  $y$  it can be easily shown that  $y = r\sqrt{k}$  where  $r \in \mathbb{Q}$  and  $k$  is square free. For uniqueness of  $k$  let  $p_1 = (r_1, r_2\sqrt{k})$  and  $p_2 = (r'_1, r'_2\sqrt{k'})$  be in the rational set  $S$ . Hence the distance between  $p_1$  and  $p_2$  is a rational number. By writing the square of the distance between two points  $p_1$  and  $p_2$  it follows that the number  $2r_2r'_2\sqrt{kk'}$  should be a rational number and hence  $\sqrt{kk'}$  is rational. Since  $k$  and  $k'$  are square free therefore we have  $k = k'$ . ■

Note that we have the following two important theorems from [SZ] :

**Theorem 3** ([SZ]) *Every rational subset of the plane has only finitely many points in common with an algebraic curve defined over  $\mathbb{R}$ , unless the curve has a line or circle as a component.*

**Theorem 4** ([SZ]) *If a rational set  $S$  has infinitely many points on a line (respectively circle) then all but 4 (respectively 3) points of  $S$  are on the line (respectively circle).*

As we see the previous two theorems give a complete description of rational distance sets with infinitely many points on a line. Hence if the Erdős-Ulam conjecture is false; i.e. there is a dense rational set in  $\mathbb{R}^2$ , then Theorem 4 implies that every line intersects  $S$  in finitely many points. The following main result in [MS] gives a uniform bound on the cardinality of these intersections.

**Theorem 5** *Assume Uniform Bound Conjecture and let  $S$  be an infinite rational subset of the plane which has finite intersection with each line. Then there exist an integer number  $B(S)$  such that for each line  $L$  in the plane the intersection  $S \cap L$  has at most  $B(S)$  points. Moreover  $B(S) \leq B(\mathbb{Q}, 2)$ , in particular there is an upper bound for  $B(S)$  independent of  $S$ .*

### 3 Proofs

Let  $A = \{(\alpha_1, \beta_1), \dots, (\alpha_m, \beta_m)\}$  be a subset of  $\mathbb{R}^2$  not all on a line and assume  $m$  is an even integer number of the form  $m = 2g + 2$  with  $g \geq 2$ . Recall that in the introduction we associate to the subset  $A$  the following surface  $X$

$$z^2 = \prod_{i=1}^m \{(x - \alpha_i)^2 + (y - \beta_i)^2\}, \quad (3.2)$$

and we called it distance surface. For finding the singularities of this surface we can rewrite the equation of the surface as follows :

$$z^2 = \prod_{j=1}^m \{(x - \alpha_j) + i(y - \beta_j)\} \{(x - \alpha_j) - i(y - \beta_j)\},$$

or equivalently we can write

$$z^2 = \prod_{j=1}^m (x + iy - (\alpha_j + i\beta_j))(x - iy - (\alpha_j - i\beta_j)).$$

Now by making the change of coordinates  $x + iy \rightarrow x$  and  $x - iy \rightarrow y$  the equation of the surface in the new coordinate is of the following form:

$$z^2 = P(x)Q(y),$$

where  $P(x) = (x - z_1) \cdots (x - z_m)$ ,  $Q(y) = (y - \bar{z}_1) \cdots (y - \bar{z}_m)$  and  $z_j = \alpha_j + i\beta_j$  for  $j = 1, \dots, m$ . Now for singularities we have to compute the partial differentials yielding the following equations:

$$z = 0, \quad P'(x)Q(y) = 0, \quad P(x)Q'(y) = 0.$$

Since these points should be on the surface and the fact that the polynomials  $P, Q$  has no multiple roots we should have

$$z = 0, P(x) = 0, Q(y) = 0.$$

So the singular points on the affine part ( $w = 1$ ) are the  $m^2$  points  $(z_i, \bar{z}_j, 0)$  for  $i, j = 1, \dots, m$ . One can easily see that the point at infinity is a singular point of the following type:

$$z^{2m-2} = x^m y^m,$$

Also the type of singularity at singular points  $(z_i, \bar{z}_j, 0)$  is of the type  $z^2 = xy$ . In the next step we show that the singular surface  $S$  with equation  $z^2 = P(x)Q(y)$  ( $P$  and  $Q$  are two polynomials of the same degree without multiple roots) is a surface of general type.

In fact the surface  $X$  is the branched double cover of the surface  $\mathbb{P}^1 \times \mathbb{P}^1$  by the morphism  $\pi : (x, y, z) \rightarrow (\frac{x}{z}, \frac{y}{z})$  which is clearly a rational morphism. This morphism is clearly branched along the locus  $z = 0$  or equivalently  $P(x)Q(y) = 0$ , that is the union of the  $2g + 2$  fibers from each ruling of  $\mathbb{P}^1 \times \mathbb{P}^1$ .

Now we can see that the surface  $X$  is a surface of general type. Hence we showed that the surface  $X$  is a singular surface with singularity at the  $m^2 = (2g + 2)^2$  points  $(z_i, \bar{z}_j, 0)$  lying over the double points of the branched divisor. We can simply write down the canonical differentials on  $X$ : if we set

$$\omega := \frac{dy \wedge dx}{z},$$

we can readily check that the products

$$\omega_{k,l} := y^k x^l \omega$$

give regular canonical differentials on the smooth locus of the surface  $X$  for all  $0 \leq k, l \leq g - 1$ . One can easily see that the ramification divisor  $R$  of  $\pi$  is the zero divisor of the function  $z$  and we have the equality

$$2R = (z^2) = (P(x)) + (Q(y)),$$

Applying the Riemann-Hurwitz formula to the cover  $\pi : S \rightarrow \mathbb{P}^1 \times \mathbb{P}^1$  on the smooth part of  $X$  we obtain:

$$\begin{aligned} K_X &= \pi^*(K_{\mathbb{P}^1 \times \mathbb{P}^1}) \otimes \mathcal{O}_X(R) \\ &= \pi^*(K_{\mathbb{P}^1 \times \mathbb{P}^1}) \otimes \mathcal{O}_{\mathbb{P}^1 \times \mathbb{P}^1}(g + 1, g + 1) \\ &= \pi^*(\mathcal{O}_{\mathbb{P}^1 \times \mathbb{P}^1}(g - 1, g - 1)), \end{aligned}$$

which is ample.

Now we need to deal with singular points of the surface  $X$ . At the singular point  $(z_i, \bar{z}_j, 0)$  after replacing  $x$  and  $y$  by  $x - z_i$  and  $y - \bar{z}_j$  respectively, the surface  $X$  will have the local equation  $z^2 = xy$ . Hence by blowing up once we obtain a smooth surface  $\tilde{X}$ . Moreover, in terms of local coordinates we have

$$z' = z, \quad x' = x/z, \quad y' = y/z$$

on  $\tilde{X}$ . The pullback of the form  $\omega$  to the surface  $\tilde{X}$  may be written as

$$\begin{aligned} \omega' &= \frac{d(y'z') \wedge d(x'z')}{z'} \\ &= z'(dy' \wedge dx') + x'(dy' \wedge dz') + y'(dz' \wedge dx'), \end{aligned}$$

which is regular on all of  $\tilde{X}$ . Thus all the forms  $\omega_{k,l}$  above pull back to regular forms on  $\tilde{X}$ . Therefore in this way we proved that the Kodaira dimension of the surface  $\tilde{X}$  (and also for the singular surface  $X$ ) is equal to 2. This complete the proof of Theorem 1. ■

Following the above theorem, we can pose the similar plausible question in  $\mathbb{R}^n$  rather than  $\mathbb{R}^2$ . But the method of the proof for the case  $\mathbb{R}^2$  can't be applied to this more generalized case.

**Question-**Let  $A = \{A_1, \dots, A_m\}$  be a finite subset of points in the  $n$ -dimensional Euclidean space not all on a hyperplane. Then can one deduce that the associated distance hypersurface (its projectivization)

$$x_{n+1}^2 = \prod_{i=1}^m ((x_1 - a_{i1})^2 + (x_2 - a_{i2})^2 + \dots + (x_n - a_{in})^2) \quad (3.3)$$

in  $\mathbb{P}^{n+1}$  is of general type?

**Remark 1** *By the above theorem we can in fact generate surfaces of general type of arbitrary degree  $d \geq 12$  in the projective space  $\mathbb{P}^3$ .*

Now we can prove Theorem 2 which answers the question asked by Ulam and Erdős.

**Proof of Theorem 2** - We apply Theorem 1 to resolve Ulam conjecture. Assume  $S \subset \mathbb{R}^2$  is a dense rational distance subset of the plane and also assume that  $(0, 0), (1, 0) \in S$ . By lemma 2 there exists a square free integer  $k$  for which the points in  $S$  are of the form  $(a, b\sqrt{k})$ , where  $a, b \in \mathbb{Q}$ . Since  $S$  is dense we can choose 6 points  $A = \{(a_1, b_1\sqrt{k}), \dots, (a_6, b_6\sqrt{k})\}$  in general position in  $S$ . Let  $X$  be the distance surface associated to the subset  $A$  which is given by the equation

$$z^2 = \prod_{i=1}^6 \{(x - a_i)^2 + (y - b_i\sqrt{k})^2\}, \quad (3.4)$$

and it is clearly defined over the number field  $K = \mathbb{Q}(\sqrt{k})$ . By the Theorem 1 we know that the surface  $X$  defined over  $K$  is a surface of general type and assuming Bombieri-Lang conjecture the  $K$ -rational points on  $X$  can not be Zariski dense. Now since  $S$  is dense in  $\mathbb{R}^2$  it is in fact Zariski dense in  $\mathbb{C}^2$  and so is dense in  $\mathbb{P}^1 \times \mathbb{P}^1$ . On the other hand the surface  $X$  is birationally the double cover of the surface  $\mathbb{P}^1 \times \mathbb{P}^1$  by the map  $(x, y, z) \rightarrow (\frac{x}{z}, \frac{y}{z})$ , and so the dense set  $S$  generates a Zariski-dense set of  $K$ -rational points in the surface  $X$  which contradicts the Bombieri-Lang conjecture. ■

**Proof of Corollary 1** - As we see in the proof of Theorem 2 the set  $S$  is not Zariski dense in  $\mathbb{R}^2$ . Hence  $S$  should be contained in the union of finitely many irreducible algebraic curves  $C_1, \dots, C_n$  in the plane. According to Theorem 3 lines and circles are the only irreducible algebraic curves that contain an infinite rational set, so one of the irreducible curves  $C_i$  should be a line (circle) with infinitely many points of rational set  $S$  and according Theorem 4 all but 4 (resp. 3) points of  $S$  are on the line (resp. circle). ■

I believe that if the points in the subset  $A = \{(\alpha_1, \beta_1), \dots, (\alpha_n, \beta_n)\}$  are chosen generically then the rational curves in the corresponding distance surface  $S : z^2 = P(x)Q(y)$  are contained in the subvariety  $D = \{z = 0\} \subset S$ . This problem is interesting enough to be dealt with in a future research.

In the final step of preparation of this paper I noticed that Terence Tao has given another conditional proof of this problem in his weblog which is more difficult than mine. In fact his example for a surface of general type is a complete intersection of 4 hyper-surfaces in  $\mathbb{C}^6$ .

**Acknowledgement-** I would like to thank Professor Tao for giving me some instructive comments that improved the original version of this paper and suggesting me to publish this result. I am also grateful to M. Makhul who brought to my attention this problem and many stimulating discussions. I also thank K. Shokri for reading the first draft and useful suggestions. The author was supported by a grant from Shahid Beheshti University.

## References

- [AE] N.H. Anning and P. Erdős, *Integral distances*, Bull. Amer. Math. Soc., (1945) 51, 598–600.
- [BMP] P. Brass, W. Moser, and J. Pach, *Research Problems in Discrete Geometry*. Springer, Berlin. 1st ed. (2005).
- [CHM1] L. Caporaso, J. Harris and B. Mazur, *Uniformity of rational points*. J. Amer. Math. Soc. (1997) **10**, 135.
- [CHM2] L. Caporaso, J. Harris and B. Mazur, *How many rational points can a curve have?*, The moduli space of curves (Texel Island, 1994), Progr. Math. **129**, Birkhuser Boston, MA, (1995), 13 - 31.
- [Ca1] L. Caporaso, *Counting rational points on algebraic curves*, in: Number Theory, I (Rome, 1995), Rend. Sem. Mat. Univ. Politec. Torino 53 (1995), 223 - 229.



- [Ca2] L. Caporaso. *Distribution of rational points and Kodaira dimension of fiber products*. In *The moduli space of curves* (Texel Island, 1994), volume 129 of Progr. Math. (1995) pages 1 - 12. Birkha user Boston,
- [E] P. Erdős, *Some combinatorial and metric problems in geometry*, Colloquia Mathematica Societatis János Bolyai 48 . Intuitive Geometry, Siófok, (1985) 167-175
- [G] R. Guy, *Unsolved Problems in Number Theory* Problem Books in Mathematics Subseries: Unsolved Problems in Intuitive Mathematics , Vol.1, Springer, 3rd ed., (2004).
- [H] G. Huff, *Diophantine problems in geometry and elliptic ternary forms*, Duke Math. J. (1948) 15 , 443 - 453.
- [K] A. Kemnitz. *Punktmengen mit ganzzahligen Abständen*, Habilitationsschrift, TU Braunschweig, 1988.
- [L] S. Lang, *Hyperbolic and Diophantine analysis*. Bull. Amer. Math. Soc. (1986) 14, 159 - 205.
- [MS] M. Makhul, J.Shaffaf, *On uniform boundedness of a rational distance set in the plane*, Comptes Rendus Mathematique, (2012) Vol. 350, 121- 124.
- [P] W. Peeples , *Elliptic curves and rational distance sets*, Proc. Amer. Math. Soc. 5 (1954), 29 - 33.
- [SZ] J. Solymosi and F. de Zeeuw, *On a question of Erdős and Ulam*, Discrete Comput. Geom. **43** (2010), no. 2, 393 - 401.
- [S] J. Solymosi, *Note on integral distances*. Discrete Comput. Geom. (2003) 30(2), 337 - 342.
- [U] S.M. Ulam, *A Collection of Mathematical Problems*, Interscience Tracts in Pure and Applied Mathematics, Number 8. Interscience Publishers (1960).

DEPARTMENT OF MATHEMATICAL SCIENCES, SHAHID BEHESHTI UNIVERSITY, G.C., P.O.Box 1983963113, TEHRAN, IRAN.

EMAIL: *J-Shaffaf@sbu.ac.ir*